

Serial No. 09/636,393

PATENT  
Docket No. PU050092

AF  
Dey



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	N. Allibhoy et al.	Examiner:	J. Reagan
Serial No.	09/636,393	Group Art Unit:	3621
Filed:	August 9, 2000	Docket No.	PU050092
Title:	A METHOD AND SYSTEM FOR CONTROLLING AND AUDITING CONTENT/SERVICE SYSTEMS		
Customer No.:	24498		

---

**APPELLANT'S BRIEF**

MAIL STOP: APPEAL BRIEF - PATENTS  
Commissioner for Patents  
Post Office Box 1450  
Alexandria, Virginia 22313-1450

Sir:

This appeal brief is being filed in response to the Notice of Appeal filed on January 11, 2010. Appellants request a four month extension under 37 C.F.R. 1.136(a) to submit this response. Appellants also request that the \$540.00 fee for filing this appeal brief and the fee for the four month extension be charged to Deposit Account 07-0832.

Appellants do not request an oral hearing.

**I. REAL PARTY IN INTEREST**

The real party in interest in this appeal is Thomson Licensing Inc., the assignee of record.

07/23/2010 HBELETE1 00000067 070832 09636393  
01 FC:1402 540.00 DA

## **II. RELATED APPEALS AND INTERFERENCES**

There are no appeals or interferences that will directly affect, or be directly affected by, or have a bearing on the Board's decision in this appeal.

## **III. STATUS OF CLAIMS**

The status of claims of all the claims in the application, Claims 1-19, is set forth in Appendix A of this brief.

Claims 13 and 16-17 are cancelled.

Claims 3-7, 14-15, and 42-50 are effectively cancelled because the rejections to such claims are not being appealed.

Claims 2, 8-12 and 18-41 are pending.

Claims 2, 8-12 and 18-41 are rejected under U.S.C. § 103(a).

Rejections to Claims 2, 8-12 and 18-41 are being appealed in this brief.

## **IV. STATUS OF AMENDMENTS**

All amendments to the claims have been entered in and are reflected in Appendix A.

## **V. SUMMARY OF CLAIMED SUBJECT MATTER**

Claim 1 claims a method for a content provider (105) to send enhanced content (additional information about a topic currently being broadcasted, information about an item currently being shown, on demand program, and the like, page 9, lines 18-22 of the specification) to a receiver (103), where a network operator (101) controls the network and the financial transaction that is made between the receiver and content provider (page 6, lines 18-29 of the specification). When a receiver issues a request for enhanced content, the request is intercepted by a third party, which is not the content provider, using software

such as the ATV software present in the receiver (steps 203 and 207, page 9, lines 25-29, page 16, lines 8-10, page 22, lines 19-22 of the specification).

In this step, a determination is made whether the content provider referenced in the intercepted request is authorized to deliver the requested content (209, specification page 9, lines 29-30 of the specification). When the content provider is not authorized, the transmission of such requested enhanced content will be prevented (steps 211, 213, page 10, lines 1-4). The method concludes with the third party storing information about the transaction, when such content is transmitted (step 251, page 13, lines 4-6 of the specification).

Claim 2 provides an additional method step where the request for requested content will be rerouted to an authorized content provider, by the third party, if the request was directed towards an unauthorized content provider (step 217, page 10, lines 3-5 of the specification).

Claim 8 discloses a method for having a network transaction being monitored between a user receiver (103) and a content provider (105) through a network operator (101). A request directed toward the content provider is intercepted by a third party (steps 203, 207, page 9, lines 25-29, page 16, lines 8-10, page 22, lines 19-22 of the specification). As the request is being intercepted, parameters are appended to the user request (step 223, page 11, lines 17-22 of the specification).

A decision is then made whether or not to direct the user request with the appended

parameters to the intended content provider, provided the content provider is authorized (209, specification page 9, lines 29-30). The content is provider is authorized; the user request will proceed to go to the authorized content provider (step 251, page 13, lines 4-6 of the specification).

If the content provider is not authorized, the operations between the unauthorized content provider and the user are terminated (step 213, page 10, lines 1-2 of the specification). The user request will then be forwarded to a substitute content provider, afterwards (217, page 10, lines 3-5 of the specification).

On the return path from an authorized content provider, a user request response directed at the user receiver by the content provider will be intercepted the third party (step 233, page 11, lines 28-30 of the specification). Information will then be extracted from this intercepted user request response (steps 233, 235, page 11, line 28 to page 12, line 4 of the specification). The intercepted user request response is then relayed back to the user (step 237, page 12, lines 5-22 of the specification).

Claim 28 claims a method for controlling a network transaction, where the first step involves having enhanced broadcast content be directed to a plurality of user receivers, the network is controlled by a network operator (101) where such enhanced broadcast information comes from a content provider (105, step 201, 501, page 9, lines 15-24, page 8, lines 16-19 of the specification). While the enhanced content information is being provided by the content provider, a third party detects triggers in such content (step 219,

page 10, lines 9-12 of the specification).

The method of Claim 28 continues with having a user request being directed to at least one content provider be intercepted (steps 203 and 207, page 9, lines 25-29, page 16, lines 8-10, page 22, lines 19-22 of the specification), where such an intercepted user request gets directed by a third party controller (step 207, page 9, lines 27-29 of the specification). While the user request is being directed, third party parameters are added to the user request (steps 205, 513 page 9, lines 25-27, page 19, lines 8-13 of the specification).

The user request with the additional third party parameters will be directed to the specified content provider if such a content provider is authorized (steps 209, 503, 507 page 9, lines 29-30, page 18, lines 19-32 of the specification). Otherwise, the adjusted user request will be redirected to an authorized content provider (steps 217, 523, page 10, lines 3-5, page 19, lines 22-24 of the specification). The method then continues with network operator adding parameters to a response (such as the transmission of enhanced content) to the user request (step 531, page 20, lines 4-6 of the specification). The response to the user request is then directed to the user receiver whereby the added parameters to the response are detected by the third party controller (step 531, page 20, lines 6-8 of the specification). The transaction information provided by the content provider in such a response is then stored (steps 251, 533, page 13, lines 4-6, page 20, lines 9-13 of the specification).

**VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL**

Claims 2, 8-12 and 18-41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ben-Shaul et al. (U.S. Patent Application No. 2002/0010798, hereafter referred to as 'Ben-Shaul') and in view of Stefik et al. (U.S. Patent 6,895,392B2, hereafter referred to as 'Stefik').

**VII. ARGUMENT****A. REJECTION OF CLAIMS 2 UNDER 35 U.S.C. § 103(a)**

The Office Action rejected dependent Claim 2 (which depends on Claim 1) under 35 U.S.C. § 103(a) as being anticipated by Ben-Shaul and in view of Stefik. However, as will be discussed, neither Ben-Shaul nor Stefik provide a teaching for this claim.

1. In the rejection, the Examiner cites to Ben-Shaul as teaching the claimed element of "permitting the enhanced content programming to be provided to the receiver over the network in response to the user request *only if the content provider is an authorized content provider of the third party*" (emphasis added). Specifically, the Examiner cites to paragraph 0426 of Ben-Shaul (with Stefik) as teaching this claimed feature. The text of paragraph 0426 is produced below:

"It is possible, however, that the content provider permits downloading of such content only after the user *requesting the material has been authorized* or otherwise properly identified. For example, free software is typically given after a proper form has been completed. In such a case the origin server 10 dynamically links the authorized user, such as the client 14 to the downloaded material after obtaining a registration or authorization. In this situation, it is normally inappropriate for the origin server 10 to remotely cache such content. Yet, since such entries are non-cacheable, the load on the origin server 10 and its latency could increase significantly" (emphasis added).

This section of Ben-Shaul discloses the opposite of what the Appellants' invention claims. That is, Ben-Shaul teaches that it is the user who needs to be authorized. In contrast, the invention of Claim 2 is about the authorization of the content provider which supplies requested content, not the user (as disclosed in Ben-Shaul). This is a fundamental

difference between the Examiner's application of the cited art and the invention of Claim 2.

2. The Examiner correctly admits in the rejection that Ben-Shaul does not disclose the claimed element of "preventing the transmission of content to said user if said content provider is unauthorized". The Examiner then cites to Stefik (in combination with Ben-Shaul) as disclosing this feature, in particular to the recitation of the "hotlist" that is referenced in page 0196 of the Stefik reference. In actuality, the recitation of a "hotlist" as in Stefik operates in conjunction with determining whether two repositories should share content between each other. The rationale being is that if two repositories are to share content, it is possible that one may be compromised, where the sharing of content between the repositories may not be secure and permits a pirate to abscond with copied material.

If one to logically apply the concept of the "hotlist" to Ben-Shaul, one would develop a system where, assuming *arguendo* with the Examiner's position, where the edge servers 214 referred to by the Examiner of Ben-Shaul would be akin to the repositories in Stefik. The idea of the hotlists would then further suggest that Ben-Shaul and Stefik would have a system where the population of the same content between different edge servers, in a content delivery network, would depend on whether or not the edge server to be populated is secure to have content transmitted to such an edge server. This has nothing to "preventing the transmission of content to said user if said content provider is unauthorized", where the content to be transmitted is meant for a particular user in response to a user request as claimed in Claim 2.

3. Claim 2 also claims a step of "said request for said content is intercepted by said third party and *rerouted* by said third party to said authorized content provider for said enhanced content programming is said user request was directed toward said unauthorized content provider," (emphasis added). The Examiner in the rejection cites to the fact that Ben-Shaul teaches the concept of redirecting a user request back to origin website if a server has failed. The actual teaching in Ben-Shaul is as disclosed in paragraph 0369 which discloses what happens when a server fails:

*“Should the edge name server 148 fail, there is a built in recovery operation. The DNS system can ignore the forwarding command in case the forwarder is not available. This is done if the directive “first” is used in the forwarding statement. When a DNS server, such as the client regional DNS server 22, recognizes the failure of the edge name server 148, it overrides the forwarding command and accesses the authoritative DNS server 26 instead. After the edge name server 148 recovers, there is an interval during which it is still ignored by the client regional DNS server 22, but after a while, the client regional DNS server 22 renews the forwarding command,”* (emphasis added).

That is, Ben-Shaul teaches the concept of taking a user request (which is directed towards a website) and redirecting such a user request to an edge server, which in theory has the same content and is closer to a user than the content provider specified in a user request. What Ben-Shaul teaches is that a request for content will NOT be forwarded to an edge server, if such an edge server is non-operation. Restating this concept, a user request will NOT be redirected if there is a problem with an edge server. This teaching contradicts what the Examiner relies on in the rejection.

To continue with the substance of this part of the rejection, the Examiner then correctly admits the Ben-Shaul does not specifically disclose preventing content transmission if a content provider is not authorized. The Examiner then relies on the teachings in Stefik to remedy this particular deficiency of Ben-Shaul, whereby the Examiner reasons in the Rejection (on page 5, second paragraph):

“Stefik, however, discloses trustworthy repositories (see at least Figures 1 and 2, item #205 as well as the associated text), hotlist repositories that are untrusted (see at least Figures 16 and 17 as well as the associated text) and redirecting of content requests away from hotlisted repositories towards alternative repositories, where the repositories are not associated with a third party. It would have been obvious to one of the ordinary skill in the art at the time of the invention to combine the content provider system of Ben-Shaul with the redirection to another repository feature of Stefik because this would, “...prevent the unauthorized and unaccounted distribution or usage of electronically published materials” (Stefik, column 1, lines 21-25)”

In the Appellants’ review of Stefik, the Applicants cannot find such a redirection operation in Stefik. Regardless of this absence, in the case in Stefik where a repository is listed on a hotlist as being untrustworthy (see step 1608), Figure 16 presents that concept



that the transaction between two repositories will be terminated (see stop 1618), not redirected as claimed by the Examiner.

Hence, when the two references are combined, the references do not disclose or suggest the claimed feature of “said request for said content is intercepted by said third party and rerouted by said third party to said authorized content provider for said enhanced content programming is said user request was directed toward said unauthorized content provider”. Assuming *arguendo* with the Examiner’s conclusions, the combination of the system of Ben-Shaul combined with Stefik either suggests that a user request for content will be directed towards the server intended in the user request when an edge server fails or a connection between two servers will be terminated if one server is on a hotlist. Regardless, both situations are in conflict with each other and do not disclose or suggest the Appellants’ invention.

**B. REJECTION OF CLAIMS 8-12 and 18-27 UNDER 35 U.S.C. § 103(a)**

The Office Action rejected Claims 8-12 and 18-27 under 35 U.S.C. § 103(a) as being anticipated by Ben-Shaul and in view of Stefik. As to be discussed, neither Ben-Shaul nor Stefik provide a teaching for this claim. Applicants will argue Claim 8 as a representative claim.

1. In the rejection, the Examiner states that when a content provider is authorized, “intercepting a user requested *response* directed at a user receiver by the content provider, wherein said user request response comprises at least a portion of the network transaction and said intercepting is performed by said third party” is taught in Ben-Shaul (in combination with Stefik). The Appellants disagree with this conclusion.

In the disclosure of Ben-Shaul, the reference involves the citation to edge servers, where user requests for content are directed towards edge servers. This obviously applies to an upstream request. The aspect of Claim 8 of “intercepting a user requested *response* directed at a user receiver” operates as having on intercept the response to a user’s receiver from an authorized content server which is a downstream interception. Appellants were not able to find such an operation in the review of either Ben-Shaul or Stefik.

2. In the rejection, the Examiner cites to Ben-Shaul as teaching the claimed element of “directing said appended user request to the content provider *if the content provider is authorized to provide enhanced content programming to the user receiver*” (emphasis added). Specifically, the Examiner cites to paragraph 0426 of Ben-Shaul (with Stefik) as teaching this claimed feature. The text of paragraph 0426 is produced below:

“It is possible, however, that the content provider permits downloading of such content only after the user *requesting the material has been authorized* or otherwise properly identified. For example, free software is typically given after a proper form has been completed. In such a case the origin server 10 dynamically links the authorized user, such as the client 14 to the downloaded material after obtaining a registration or authorization. In this situation, it is normally inappropriate for the origin server 10 to remotely cache such content. Yet, since such entries are non-cacheable, the load on the origin server 10 and its latency could increase significantly” (emphasis added).

Actually, Ben-Shaul discloses the exact opposite of what the Appellants’ invention claims. That is, Ben-Shaul teaches that it is the user that needs to be authorized. In contrast, the invention of Claim 8 is about the authorization of the content provider which supplies requested content, not the user (as disclosed in Ben-Shaul). Clearly, this is a fundamental difference between the Examiner’s cited art and the invention of Claim 8.

3. The Examiner correctly admits in the rejection that Ben-Shaul does not disclose the claimed element of “terminating the network transaction between the user receiver and the content provider if the content provider is unauthorized”. The Examiner then cites to Stefik (in combination with Ben-Shaul) as disclosing this feature, in particular to the recitation of the “hotlist” that is referenced in page 0196 of the Stefik reference. Appellants note in actuality, the recitation of a “hotlist” as in Stefik operates in conjunction with determining whether two repositories should share content between each other. The rationale being is that if two repositories are to share content, it is possible that one may be compromised, where the sharing of content between the repositories may not be secure.

If one to logically apply the concept of the “hotlist” to Ben-Shaul, one would develop a system where, assuming *arguendo* with the Examiner’s position, the edge servers 214 referred to by the Examiner of Ben-Shaul would be akin to the repositories in

Stefik. The idea of the hotlists would then infer that Ben-Shaul and Stefik would suggest a system where the population of the same website content between different edge servers, in a content delivery network, would depend on whether or not the edge server to be populated is secure to have content transmitted to such an edge server. This has nothing to “preventing the transmission of content to said user if said content provider is unauthorized”, where the content to be transmitted is meant for a particular user in response to a user request as in Claim 8.

4. Claim 8 also claims a method step of “*forwarding* said appended user request to a substitute content provider *if the content provider is unauthorized*,” (emphasis added). The Examiner in the rejection cites to the fact that Ben-Shaul teaches the concept of redirecting a user request back to origin website if a server has failed. The actual teaching in Ben-Shaul is in paragraph 0369 that describes what happens when a server fails:

*“Should the edge name server 148 fail, there is a built in recovery operation. The DNS system can ignore the forwarding command in case the forwarder is not available. This is done if the directive “first” is used in the forwarding statement. When a DNS server, such as the client regional DNS server 22, recognizes the failure of the edge name server 148, it overrides the forwarding command and accesses the authoritative DNS server 26 instead. After the edge name server 148 recovers, there is an interval during which it is still ignored by the client regional DNS server 22, but after a while, the client regional DNS server 22 renews the forwarding command,”* (emphasis added).

That is, Ben-Shaul teaches the concept of taking a user request (which is directed towards a website) and redirecting such a user request to an edge server, which in theory has the same content and is closer to a user than the website specified in a user request. What Ben-Shaul teaches is that a request for content will NOT be forwarded to an edge server, if such an edge server is non-operation. Restating this concept, a user request will NOT be redirected if there is a problem with an edge server. This teaching contradicts what the Examiner relies on in the rejection.

To continue with this part of the rejection, the Examiner then correctly admits the Ben-Shaul does not specifically disclose preventing content transmission if a content

provider is not authorized. The Examiner then relies on the teachings in Stefik to remedy this particular deficiency of Ben-Shaul, whereby the Examiner reasons in the Rejection (on page 6, fifth paragraph):

“Stefik, however, discloses trustworthy repositories (see at least Figures 1 and 2, item #205 as well as the associated text), hotlist repositories that are untrusted (see at least Figures 16 and 17 as well as the associated text) and redirecting of content requests away from hotlisted repositories towards alternative repositories, where the repositories are not associated with a third party. It would have been obvious to one of the ordinary skill in the art at the time of the invention to combine the content provider system of Ben-Shaul with the redirection to another repository feature of Stefik because this would, “...prevent the unauthorized and unaccounted distribution or usage of electronically published materials” (Stefik, column 1, lines 21-25)”.

In the Appellants’ review of Stefik, the Applicants cannot find such a redirection operation in Stefik. Regardless of this absence, Stefik teaches that when a repository is listed on a hotlist as being untrustworthy (see step 1608), the transaction between two repositories will be terminated (see stop 1618), not redirected as claimed by the Examiner.

Hence, when the two references are combined, the references do not disclose or suggest the claimed feature of “said request for said content is intercepted by said third party and rerouted by said third party to said authorized content provider for said enhanced content programming is said user request was directed toward said unauthorized content provider”. Assuming arguendo with the Examiner’s conclusions, the combination of the system of Ben-Shaul combined with Stefik either suggests that a user request for content will be directed towards the server intended in the user request when an edge server fails or a connection between two servers will be terminated if one server is on a hotlist. Regardless, both situations are in conflict with each other and do not disclose or suggest the Appellants’ invention.

### **C. REJECTION OF CLAIMS 28-41 UNDER 35 U.S.C. § 103(a)**

The Office Action rejected Claims 28-41 under 35 U.S.C. § 103(a) as being anticipated by Ben-Shaul and in view of Stefik. However, as will be discussed, neither Ben-Shaul nor Stefik provide a teaching for this claim. Applicants will argue Claim 28 as a representative claim.

1. In the rejection, the Examiner states that when a content provider is authorized, “*detecting triggers within said portion of said enhancement broadcast information provided by said at least one content provider, wherein said detecting step is performed by a third party*” is taught in Ben-Shaul (in combination with Stefik). The Appellants disagree with this conclusion.

Within the disclosure of Ben-Shaul, the reference involves the citation to edge servers, where user requests for content are directed towards edge servers. This obviously applies to an upstream request. The aspect of Claim 28 of “detecting triggers within said portion of said enhancement broadcast information provided by said at least one content provider” operates as the detection of triggers from a content provider to a user’s receiver, where such a detection is done by a third party. Appellants were not able to find such a downstream operation in the review of either Ben-Shaul or Stefik.

2. In the rejection, the Examiner cites to Ben-Shaul as teaching the claimed element of “directing said appended user request to the content provider *if the content provider is authorized to provide enhanced content programming to the user receiver*” (emphasis added). Specifically, the Examiner cites to paragraph 0426 of Ben-Shaul (with Stefik) as teaching this claimed feature. The text of paragraph 0426 is produced below:

“It is possible, however, that the content provider permits downloading of such content only after the user *requesting the material has been authorized* or otherwise properly identified. For example, free software is typically given after a proper form has been completed. In such a case the origin server 10 dynamically links the authorized user, such as the client 14 to the downloaded material after obtaining a registration or authorization. In this situation, it is normally inappropriate for the origin server 10 to remotely cache such content. Yet, since such entries are non-cacheable, the load on the origin server 10 and its latency could increase significantly” (emphasis added).

Ben-Shaul discloses is actually the exact opposite of what the Appellants’ invention claims. That is, Ben-Shaul discloses that it is the user that needs to be authorized. In contrast, the invention of Claim 28 is about the authorization of the content provider which supplies requested content, not the user (as disclosed in Ben-Shaul). This is a fundamental difference between the Examiner’s cited art and the invention of Claim 28.

3. The Examiner correctly admits in the rejection that Ben-Shaul does not disclose the claimed element of “redirecting said user request to an authorized content provider if it is determined that said at least one content provider is not authorized”. The Examiner then cites to Stefik (in combination with Ben-Shaul) as disclosing this feature, in particular to the recitation of the “hotlist” that is referenced in page 0196 of the Stefik reference, where in the

Specifically, the Examiner in the rejection cites to the fact that Ben-Shaul teaches the concept of redirecting a user request back to origin website if a server has failed. The actual teaching in Ben-Shaul is as disclosed in paragraph 0369 as reproduced below which is what happens when a server fails:

*“Should the edge name server 148 fail, there is a built in recovery operation. The DNS system can ignore the forwarding command in case the forwarder is not available. This is done if the directive “first” is used in the forwarding statement. When a DNS server, such as the client regional DNS server 22, recognizes the failure of the edge name server 148, it overrides the forwarding command and accesses the authoritative DNS server 26 instead. After the edge name server 148 recovers, there is an interval during which it is still ignored by the client regional DNS server 22, but after a while, the client regional DNS server 22 renews the forwarding command,”* (emphasis added).

That is, Ben-Shaul teaches the concept of taking a user request (which is directed towards a website) and redirecting such a user request to an edge server, which in theory has the same content and is closer to a user than the website specified in a user request. What Ben-Shaul also teaches is that a request for content will NOT be forwarded to an edge server, if such an edge server is non-operational. Instead, a user request will be directed to the originally requested server in a user request.

To continue with the substance of this part of the rejection, the Examiner then argues that Ben-Shaul does not specifically disclose preventing content transmission if a content provider is not authorized. On its face, this aspect of the rejection does not matter as the claim language of Claim 28 does not claim this specific feature.

Assuming arguendo for the Examiner’s point and for allowing for prosecution of this application to proceed, the Applicants assume the Examiner meant to argue that Ben-

Shaul does not specifically disclose the concept of determining whether or not a content provider is authorized, where such a user request would be redirected to an authorized content provider. Ben-Shaul however does not disclose of having some operation occur if a content provider is deemed to be unauthorized.

The Examiner then relies on the teachings in Stefik to remedy this particular deficiency of Ben-Shaul, whereby the Examiner reasons in the Rejection (on page 9, third paragraph):

“Stefik, however, discloses trustworthy repositories (see at least Figures 1 and 2, item #205 as well as the associated text), hotlist repositories that are untrusted (see at least Figures 16 and 17 as well as the associated text) and redirecting of content requests away from hotlisted repositories towards alternative repositories, where the repositories are not associated with a third party. It would have been obvious to one of the ordinary skill in the art at the time of the invention to combine the content provider system of Ben-Shaul with the redirection to another repository feature of Stefik because this would, “...prevent the unauthorized and unaccounted distribution or usage of electronically published materials” (Stefik, column 1, lines 21-25)”.

In the Appellants’ review of Stefik, the Applicants cannot find such a redirection operation in Stefik. Rather, Stefik discloses that when a first repository is listed on a hotlist as being untrustworthy during the communication between two repositories (see step 1608), such a communications will be terminated (see step 1618). This is not the redirection cited to by the Examiner as being in Stefik. Hence, when the two references are combined, the references do not disclose or suggest the claimed feature of “redirecting said user request to an authorized content provider if it is determined that said at least one content provider is not authorized”. Assuming *arguendo* with the Examiner’s conclusions, the combination of the system of Ben-Shaul with Stefik either suggests that a user request for content will be directed towards the server intended in the user request when an edge server fails or a connection between two servers will be terminated if one server is on a hotlist. Regardless, both situations are in conflict with each other and do not disclose or suggest the Appellants’ invention.

**VIII. CLAIMS APPENDIX**

A complete listing of the claims involved in this appeal is attached hereto as Appendix A.

**IX. EVIDENCE APPENDIX**

Appellant does not submit any additional evidence and, therefore, an Appendix B is hereby attached indicating "none."

**X. RELATED PROCEEDINGS APPENDIX**

Appellant states that there are no relevant related proceedings and, an Appendix C is hereby attached indicating "none."

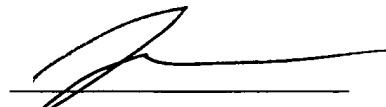
**XI. CONCLUSION**

The Examiner has not shown in the cited prior art where one may find support for rejections of the pending claims on Appeal. There is simply no disclosure/support pointed out by the Examiner that recites the features in Claims 2, 8-12 and 18-41. Appellants contend that the rejections are traversed and overcome, in light of the arguments presented above.

The allowance of all claims on Appeal is therefore respectfully requested.

Respectfully submitted,

Date: 7/12/2011



Joel M. Fogelson

Reg. No 43,613

Phone No. 609-734-6809



Serial No. 09/636,393

PATENT  
Docket No. PU050092

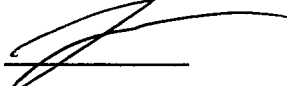
Patent Operations  
Thomson Licensing Inc.  
P.O. Box 5312  
Princeton, New Jersey 08543-  
5312

Attachments:  
Appendix A: Claims on Appeal  
Appendix B: Evidence  
Appendix C: Related Proceedings

CERTIFICATE OF MAILING

I hereby certify that this amendment is being deposited with the United States Postal Service as First Class Mail, postage prepaid, in an envelope addressed to Mail Stop Amendment, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on:

7/12/10  
Date

  
Joel M. Fogelson  
Reg. 43,613

**APPENDIX A****CLAIMS ON APPEAL**

The following is a listing of all claims, pending or canceled, incorporating all elements and revisions to date. All non-canceled claims are on appeal, canceled claims being canceled without prejudice or disclaimer.

1. (previously presented) A method of controlling a financial transaction between a receiver and a content provider occurring over a network operated by a network operator, wherein said content provider offers enhanced content programming relating to the financial transaction, the method comprising the steps of:

intercepting a user request for the enhanced content programming, said user request originating in the receiver, wherein said intercepting step is performed by a third party;

permitting the enhanced content programming to be provided to the receiver over the network in response to the user request only if the content provider is an authorized content provider of the third party and preventing the transmission of content to said user if said content provider is unauthorized, wherein said permitting step is performed by said third party; and

storing information relating to the enhanced content programming provided to the receiver in response to the user request, wherein said storing step is performed by said third party, wherein said third party is not a content provider itself for said user request.

2. (previously presented) The method of claim 1, further comprising the step of determining if the content provider is authorized by the network operator to offer enhanced content programming over the network, wherein said request for said content is intercepted by said third party and rerouted by said third party to said authorized content provider for

said enhanced content programming if said user request was directed to said unauthorized content provider.

Claims 3-7 (cancelled)

8. (previously presented) A method for monitoring a network transaction between a user receiver and a content provider, the method comprising the steps of:

- intercepting a user request directed at the content provider by the user receiver, wherein said intercepting is performed by a third party;

- appending additional parameters to said user request;

- directing said appended user request to the content provider if the content provider is authorized to provide enhanced content programming to the user receiver and performing at least one of the following steps if the content provider is unauthorized;

- terminating the network transaction between the user receiver and the content provider if the content provider is unauthorized, and

- forwarding said appended user request to a substitute content provider if the content provider is unauthorized;

otherwise if the content provider is authorized

- intercepting a user request response directed at the user receiver by the content provider, wherein said user request response comprises at least a portion of the network transaction and said intercepting is performed by said third party;

- extracting information from said intercepted user request response; and

- forwarding said user request response by said third party to the user receiver.

9. (original) The method of claim 8, further comprising the step of initially receiving enhanced content programming from the content provider within the user receiver, and

wherein said user request is formed by the step of interacting with the content provider through the user receiver.

10. (original) The method of claim 9, further comprising the step of recognizing a trigger within said enhanced content programming, said recognizing step performed prior to said step of intercepting said user request.

11. (original) The method of claim 8, wherein said step of intercepting said user request further comprises the steps of:

- appending an address to a third party controller to said intercepted user request; and
- directing said intercepted user request to said third party controller, wherein said third party controller performs said step of appending additional parameters to said user request.

12. (original) The method of claim 8, further comprising the step of appending a marker to said user request response by the content provider, wherein said third party uses said marker to intercept said user request response.

Claims 13-17 (cancelled)

18. (original) The method of claim 8, further comprising the step of storing said extracted transaction information.

19. (original) The method of claim 8, further comprising the steps of:

- initiating a purchase from the content provider by the user receiver; and
- entering said initiated purchase into a data base controlled by a third party.

20. (original) The method of claim 19, further comprising the step of displaying information pertaining to said initiated purchase on a display screen coupled to the user receiver.

21. (original) The method of claim 20, further comprising the step of displaying at least one advertisement on said display screen simultaneously with said information pertaining to said initiated purchase.

22. (original) The method of claim 21, wherein said at least one advertisement includes linking information to a specific content provider.

23. (original) The method of claim 19, further comprising the steps of:

directing a request for additional information pertaining to said initiated purchase to said content provider, wherein said directing step is performed by said third party;

receiving said additional information from said content provider by said third party;  
and

storing said additional information in said third party controlled data base.

24. (original) The method of claim 23, further comprising the steps of:

directing a request for updating information pertaining to said initiated purchase to said content provider, wherein said directing step is performed by said third party;

receiving said updated information from said content provider by said third party;  
and

storing said updated information in said third party controlled data base.

25. (original) The method of claim 19, further comprising the steps of:

requesting finalization of said initiated purchase by the user receiver;

finalizing said initiated purchase with the user receiver, wherein said finalizing step is performed by said third party, and

providing final purchase information to the content provider by said third party.

26. (original) The method of claim 25, further comprising the step of requesting finalization of said initiated purchase the user receiver, wherein said requesting step is performed prior to said finalizing step.

27. (original) The method of claim 25, further comprising the step of obtaining supplemental information from the user by said third party in order to complete said finalizing step.

28. (previously presented) A method of controlling a network transaction, the method comprising the steps of:

directing enhanced broadcast information via a network to a plurality of receivers wherein said network is controlled by a network operator, and wherein at least a portion of said enhanced broadcast information is provided by at least one content operator;

detecting triggers within said portion of said enhanced broadcast information provided by said at least one content provider, wherein said detecting step is performed by a third party;

intercepting by said third party a user request directed at said at least one content provider from a receiver of said plurality of receivers coupled to said network;

directing said intercepted user request to a third party controller;

appending third party parameters to said intercepted user request;

directing said appended user request to said at least one content provider if said at least one content provider is authorized and redirecting said user request to an authorized content provider if it is determined that said at least one content provider is not authorized;

appending third party markers to a response to said appended user request, wherein said appending step is performed by said at least one content provider;

directing said appended response to said receiver;

detecting by said third party controller said third party markers appended to said response; and

storing transaction information provided by said at least one content provider in said response, wherein said storing step is controlled by said third party controller.

29. (original) The method of claim 28, further comprising the step of appending information to said intercepted user request prior to directing said intercepted user request prior to directing said intercepted user request to said third party controller.

30. (original) The method of claim 29, wherein said information appended to said intercepted user request is comprised of a third party controller address.

31. (original) The method of claim 29, wherein said information appended to said intercepted user request is comprised of a set of receiver capabilities.

32. (original) The method of claim 29, wherein said information appended to said intercepted user request is comprised of a user profile associated with said receiver.

33. (original) The method of claim 28, said appended third party parameters comprised of a network specification.

34. (original) The method of claim 28, said appended third party parameters comprised of a receiver specification.

35. (original) The method of claim 28, said appended third party parameters comprised of a user profile associated with said receiver.

36. (original) The method of claim 28, said appended third party parameters comprised of a set of network operator business rules.

37. (original) The method of claim 28, further comprising the steps of:

- initiating a user financial transaction through said receiver with said at least one content provider;

- storing information pertaining to said user financial transaction in a third party controller data base; and

- displaying at least a portion of said stored information on a display screen coupled to said receiver.

38. (original) The method of claim 37, further comprising the step of displaying at least one advertisement on said display screen simultaneously with said portion of said stored information.

39. (original) The method of claim 38, wherein said at least one advertisement includes linking information to a specific content provider.

40. (original) The method of claim 28, further comprising the steps of:

- requesting additional information on said user financial transaction from said at least once content provider, wherein said requesting step is performed by said third party controller;

- receiving said additional information from said at least one content provider; and
- storing said additional information.



41. (original) The method of claim 28, further comprising the steps of:

finalizing said user financial transaction through said receiver, wherein said step of finalizing is executed between said receiver and said third party controller; and

providing finalized user financial transaction information to said at least one content provider by said third party controller.

Claims 42-50 (cancelled)

**APPENDIX B**

**EVIDENCE**

None.

**APPENDIX C**

**RELATED PROCEEDINGS**

None.